



■ PhonEX™ ONE

White Paper - System Security



Table of Contents

EXECUTIVE SUMMARY	1
System Overview	1
Fully Web-based Solution	1
SYSTEM SECURITY	2
Purpose	2
Management, Control and Security.....	2
Security Groups.....	2
Directory Authentication	3
Web Security	3
Database Security	4
SYSTEM MANAGEMENT	5
System Logs.....	5
Status Monitor	5
Maintenance Tools	5
CONCLUSION	6
CONTACT INFORMATION	7

Executive Summary

Founded in 1995, MIND CTI Ltd. is a public company (NASDAQ: MNDO), a leading global provider of Call Management solutions to the enterprise market, and Billing and Customer Care solutions to the xSP market. MIND provides sales and support to its worldwide customers from offices in the United States, UK, Romania and Israel. With 300 employees and an experienced management team, MIND has a strong balance sheet and profitable operations.

MIND has a proven record in call management and accounting solutions since 1995. Through continuous research and development, MIND delivers state-of-the-art technology and advanced solutions that enable enterprises to manage, control, track, alert, budget and analyze their total telecommunication expenses and productivity. For companies that are aware of the importance and benefits of advanced call accounting and network management systems, MIND Call Management Solutions offer the most comprehensive, relevant and up-to-date solution.

System Overview

PhonEX ONE is a comprehensive, flexible and fully web-based solution for call accounting management and control. It provides an intelligent tracking of all the traditional and VoIP calls, cellular activity, and data traffic. PhonEX ONE is scalable from a single site to monitoring call traffic in multinational organizations, as it can easily be adjusted to local languages and currencies. PhonEX ONE offers powerful reports in a system that runs itself, ensuring a quick return on investment and long-term usage. PhonEX ONE helps enterprises to reduce operational costs, improve employee productivity, monitor network activity, report usage trends and statistics, and optimize network resources.

PhonEX ONE's unsurpassed powerful query generator provides up-to-the-minute customized reports and graphs giving a total, centralized view of communication networks, allowing a comparative call and data analysis, strategic planning, auditing and reconciliation of the communication resources.

From the moment PhonEX ONE is installed, organizations are able to set budgets for different departments and projects, define taxes for special calls or differential tariffs for special days or periods, reduce telephone and bandwidth expenses, prevent telephone misuse by increasing employee awareness of efficient telephone use, and ensure that IP network resources are managed effectively.

Fully Web-based Solution

PhonEX ONE is a true web-based call management solution that enables managers and users to conveniently configure, administer, rate and access their telecommunication system at anytime and from anywhere. PhonEX ONE is designed using the Microsoft .Net technology and has extensive configuration capabilities using XML files with Server - Client interaction. The SSL encryption protects the security of all sessions' passwords, thus ensuring the safety of the administrators' and user's information.

System Security

Purpose

This White Paper illustrates in detail the PhonEX ONE security enhancements and lists all user security changes that were made from the previous PhonEX ONE release.

Management, Control and Security

PhonEX ONE is designed to enable a smooth and easy management and control over the system. PhonEX ONE controlling entity is the Administrator. The Administrator is in charge of all the system's rules and tables. The Administrator manages and controls all the system's users throughout the entire organization. PhonEX ONE enables the following abilities:

- The system's rules may be configured only by the administrator, having view/edit/delete permissions.
- The Administrator may manage and restrict users from having certain privileges.
- Users have their own privileges and security groups. Sensitive features can be disabled for selected users.
- The Administrator is provided with full control for managing users easily. Using an online view of each of the users' status, each change in any of the tables' status (add, remove, import) is immediately written into the system log event and generates a detailed audit trail.
- Support for unlimited levels of web users accounts to accommodate complex organizational and business models. This ability makes it easier to define and manage accounts or P&L (Profit and Loss) units by allowing an unlimited hierarchy within the organization's structure and an unlimited number of system rules allocated to users or user groups. This ability suits not only large enterprises, but also SMEs with a complex hierarchy of web users.

Security Groups

The PhonEX ONE application provides security features that limit all or part of the program to authorized personnel only. The security features can be used to deny access of non-authorized personnel to the PhonEX ONE system parameters, to the PhonEX ONE database, and to specific reporting features. Seven default policies are available:

- Administrators
- Employee
- No rights
- Operator
- PhonEX ONE IM
- Reports Only
- Unit Manager

The PhonEX ONE security system allows each user only as much access as necessary to operate that user's part of the program. In other words, you can define the extent to which each user can access the system and database.

In addition, PhonEX ONE has a tool that allows defining custom policies – through a wizard that scans all the system entities (reports, hierarchical levels and units, employees, extensions, system tools, etc.) upon which the access can be granted or denied.

Directory Authentication

PhonEX ONE provides two ways of managing the system's users: system authentication and directory authentication. The users list can be managed and maintained in PhonEX ONE by the administrator users. This system authentication option is recommended when small number of users is used. In addition, PhonEX ONE provides the option of authenticating users against the organizational directory as **Active Directory, Lotus notes, Netscape directory** or any other LDAP directory. In this case users are authenticated and authorized against the organizational directory while policy rights groups binding is done in the background, so that users are automatically logged in with their rights. This option is preferred as a manner of work when large number of users has to be maintained.

Web Security

The enhanced user security features make PhonEX ONE a perfect solution for the enterprise environment. PhonEX ONE allows online users to access the system from a Web browser anywhere. To maximize the access security, PhonEX ONE uses a Secured Socket Layer protocol (SSL) that provides data encryption, server authentication and message integrity for a TCP/IP connection between the Microsoft Internet Information Server service protocols (SHTTP) and the browsers. The scope of this technology includes key exchange, encryption, message integrity and messaging support for authenticating a remote party using a security model that is based on digital certificates and certificate authorities. Certificate Authorities (CA) can either be a third-party such as **Verisign** or **Thawte**, or exist internally.

Whether the CA exists internally or externally, its function is to serve as a trusted authority that issues and verifies the validity of the digital certificate. The SSL on the IIS web server platform provides secure end-to-end encrypted communications between the PhonEX ONE web server and the users' Internet Explorer, which has built-in SSL functionality.

In addition to the protocol level security, there are some more features that support the security of the Web applications, such as:

- Tiered security interface, which allows the complete control over the access rights
- Encrypted passwords, which consist of a minimum of 6 alphanumeric characters
- Passwords are disabled after x consecutive attempts; detailed log events are generated, allowing the Administrator to easily track such attempts
- PhonEX ONE supports system segregation and security administration

Database Security

All the sensitive information and restricted data (such as customer passwords) are stored encrypted in the database, since the Database security is one of the most vital components of the overall security requirements. PhonEX ONE uses the Microsoft Frameworks security functionality. The static password authentication information is protected by cryptographic hash algorithms, safe from hacking or removal.

System Management

System Logs

The PhonEX ONE system stores the most recent actions regarding the system use. It shows when the system was used and who used it. The Event Log viewer is an effective management tool based on the Microsoft Event Viewer, a system administrator that can easily observe and track the system's suspicious behavior.

All the important operations performed by the user are logged. The term "important operations" includes all logins, logoffs, failed attempts to provide the correct password - that lead to account suspending, operations dealing with the database (insert/update/delete). The information in the log file will include the date/time, the IP and the message about the operation performed.

The default log level is considered to be WARNING. The Administrator (the user that has rights for the Administration rules of PhonEX ONE) can change this level. Only events of this level and up are written in the log event. For example, if the selected level is WARNING, the events with VERBOSE level are not logged, while the CRITICAL and WARNING ones are.

Status Monitor

Users and system administrators are able to view the system's status online. The Monitor displays the real time status of different system elements, providing information on disconnections, errors, processes and all other changes in the system. Whenever a problem occurs, it is immediately shown on the monitor.

The Monitor is an essential tool to audit and control the system's behavior and to observe the system's faults the minute they happen. The monitor displays the real time status of different system elements, providing information on disconnections, errors, processes and all other changes in the system. Some of the statuses shown are: Data sources, Data process, Scheduler, New Trunk Groups etc.

Maintenance Tools

The Maintenance tool is essential for debugging and working with the PhonEX ONE database. This feature is thought to be of great help for the system administrators who maintain the database. Another feature is the automatic maintenance using the system's scheduler. All the actions performed with the Maintenance tools are enabled for the Administrator user rights only. The **Maintenance** module will allow the administrator to perform several actions such as: Backup all, Delete items, Delete records and Restore.

Conclusion

The PhonEX ONE security is part of the end-to-end solution MIND provides to all kinds of enterprises and business models. The security options offer the ability to suite organizations of any size with a variety of security regulations.

The enhanced system security features facilitate the system's management and maximize the work of every system operator, while keeping it simple and effective.

The web interface centralizes maintenance to a single location. This ensures that future enhancements are performed in one location instead of across multiple individual machines. This enables the users to scale up as the network and business grow.

About MIND

MIND CTI (NASDAQ: MNDO) is a leading global provider of true web based call management and call accounting solutions. As one of the first call accounting application developers in 1995, MIND is recognized as a world leader in this field, with over 16,000 installations. A pioneer in call accounting and management solutions, MIND uses its innovative technologies to keep you at pace with the world's changing networks and requirements. MIND CTI operates from offices in the United States, UK, Romania, with headquarters in Israel. MIND offers an easy to use call accounting solution for you to manage, control and measure your telecommunications expenses and resources. For information about MIND and its products visit the company's web site: <http://www.mindcti.com/enterprise>.

How to contact us:

E-mail: sales@mindcti.com

Headquarters:

MIND CTI Ltd.
POB 144
Yoqneam Ilit, 20692, Israel
Phone: +972-4-993-6666
Fax: +972-4-993-7776

U.S. Office:

MIND Software Inc.
12520 Prosperity Drive, Suite 220
Silver Spring, MD 20904, USA
Phone: +1-301-572-1100
Fax: +1-301-586-8680
Toll Free (US): +1-877-736-8674

U.K. Office:

Parkview
Arlington Business Park
RG7 4TY, UK 1210
Tel: +44 (0)118 965 7890
Fax: +44 (0)118 965 7889

Romania Office:

MIND Software Srl.
Str. Ciurchi Nr. 126 - 128
Tudor Office Center
Iasi, 700366, Romania
Phone: +40-332-450450



THE PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO: THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THE PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. MIND CTI LTD. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

THIS DOCUMENT IS CONFIDENTIAL AND PROPRIETARY AND IS THE EXCLUSIVE PROPERTY OF MIND CTI LTD. AND HAS BEEN PROVIDED FOR REVIEW BY THE RECIPIENT ONLY, AND MAY NOT BE DISCLOSED TO ANY THIRD PARTY. INFORMATION IN THIS DOCUMENT MAY BE SUBJECT TO CHANGE WITHOUT PRIOR NOTICE. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS WHATSOEVER ELECTRONICALLY OR MECHANICALLY FOR ANY PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF MIND CTI LTD